Financial Information Security

or

"On-Guard" Everywhere (Especially the Internet)

James M. Brundy
January 19, 2002

1. Internet Security Issues for Financial Institutions

1.1. Internet is inherently less secure than other means of remote communication.

1.1.1. Internet is a "packet-switched" network and is easier to penetrate than a private-line or software-defined private network.
1.1.2. World Wide Web servers that host sites have been shown to contain security lapses. Although "fixes" exist for most of these, the fixes are by no means universally installed.
1.1.3. World Wide Web browsers are easily attacked by "trojan horse" software that permits intruders to gather, e.g., password, account number and other private information from browsers in everyday use.

1.2. Known Security Issues[1]

1.2.1. Card number theft: penetration of several e-commerce sites resulting in theft of thousands of credit card numbers.
1.2.2. Identity theft: someone obtains the necessary information to pass themselves off as another... usually resulting in financial losses. The consequences often are expensive and time-consuming to correct.
1.2.3. Hacking of business, governmental and university computer systems.
1.2.4. Financial institutions ("**FI**'s") are common and well-known targets for hackers, as "they're where the money is."

1.3. Financial Institution "Strategic Alliances."

1.3.1. **FI**s tend to lack sufficient expertise to bring their services to the Internet without assistance of outside specialists.

[1] Unlawful and undesirable conduct on the Internet is described in detail in PRESIDENT'S WORKING GROUP ON UNLAWFUL CONDUCT ON THE INTERNET, THE ELECTRONIC FRONTIER: THE CHALLENGE OF UNLAWFUL CONDUCT INVOLVING THE USER OF THE INTERNET (2000).

1.3.2. Some **FI**s have had difficulty creating sufficiently rewarding environments to attract entrepreneurial, highly skilled and creative Internet technicians.

1.3.3. Creating "strategic alliances" with entrepreneurial companies provides **FI**s with access to Internet technologies and product suites that otherwise would be inaccessible.

1.3.4. "Strategic alliances" with these "dot.coms" have involved equity stakes by **FI**s, a practice that changes the dynamic from "vendor/ buyer" to "business partners." The **FI** acquiring services may be both advantaged, e.g., by closer collaboration, and disadvantaged, e.g., by the tendency to overlook matters that would have been taken seriously in the traditional environment.

1.4. "Outsourcing" as a Way of Life

1.4.1. New service innovation: Not typical to see wholly new services created by **FI**'s

- **FI** core business is delivery of financial services, not software development and computer services; lack of technical and managerial expertise
- Necessity of "critical mass." No single **FI** may have sufficient business to achieve profitability in a reasonable time – a vendor can achieve greater volume more quickly by serving multiple competitors.
- Spreading of development expense among many competitors
- Banks internal procedures tend to be cumbersome, impeding R&D activities.

1.4.2. Provision of infrastructure

- Even for **FI** infrastructure services that are not "new," 3rd parties may have advantages over **FI**'s.
- Economies of scale in development and perhaps in processing.
- Vendor focus on a particular line of business
- Management expertise geared to that business line, not to financial product sales and service.
- These and other factors may result in a lower price for the "outsourced" service than **FI**'s cost of producing the service itself.

2. FI Risks from Outsourcing

2.1. On November 28, 2000, the Federal Financial Institutions Examination Council ("FFIEC") issued guidance on risk management of technology outsourcing.[2]

[2] Federal Financial Institutions Examination Council ("FFIEC"), Press Release and Statement, Risk Management of Outsourced Technology Services, November 28, 2000.

2.2. The FFIEC stated that it expects the boards of directors and senior management of **FI**s to oversee and manage outsourcing relationships. **FI**s were advised that they should institute an outsourcing process that includes:

2.2.1. a risk assessment to identify the **FI**'s needs and requirements;
2.2.2. proper due diligence to identify and select a provider;
2.2.3. written contracts that clearly outline duties, obligations and
2.2.4. responsibilities of the parties involved; and
2.2.5. ongoing oversight of outsourcing technology services.[3]

2.3. The FFIEC guidance encourages managers to consider additional risk-management controls when services involve the use of the Internet. The Internet, with its broad geographic reach, ease of access and anonymity, requires **FI**s' close attention to maintaining secure systems, detecting intrusions, developing reporting systems and verifying and authenticating customers.[4]

2.4. More recently, the Office of the Comptroller of the Currency ("OCC") has outlined generally the risks that may arise from business relationships with 3rd parties in general and prescribed policies for managing those risks.[5] This guidance applies as a legal matter only to national banks, but is functionally applicable to **FI**'s generally.

2.5. The risks are

2.5.1. "Strategic" – risk arising from adverse business decisions or improper implementation of those decisions. These risks can arise

- when an **FI** uses a 3rd party to conduct functions or offer services incompatible with the **FI**'s strategic goals or that do not provide adequate return on investment;
- if the **FI** fails to perform due diligence or to install adequate risk management and oversight capabilities;
- if management lacks adequate expertise and experience to oversee the 3rd -party activities properly.[6]

2.5.2. "Reputation" – risk arising from negative public opinion, including

- third-party relationships not meeting **FI** customer expectations;
- poor service, disruption of service, inappropriate sales recommendations , violations of consumer law;
- publicity about adverse events surrounding the 3rd parties.[7]

2.5.3. "Compliance" – risk resulting from violations or law or nonconformity with internal policies and procedures or ethical standards, including

---

[3] FFIEC Press Release, Risk Management of Outsourced Technology Services, November 28, 2000 at 1.
[4] Id.
[5] OCC Bulletin 2001-47, Risk Management Principles for Third-Party Relationships, November 1, 2001.
[6] Id., p. 4.
[7] Id.

- third -party services, systems or operations are inconsistent with such norms;
- failure to protect privacy of consumer and customer records;
- conflicts of interest exist between the **FI** and the 3rd party; and
- lack of an appropriate information security program.[8]

2.5.4. "Transaction" – risk from problems with service or product delivery, including

- third party services, delivery channels and processes do not fit with **FI**'s systems, customer demand or strategic objectives; and
- lack of effective business resumption and contingency operations planning.[9]

2.5.5. "Credit" – failure of an obligor to fulfill any contract or otherwise to perform as agreed, including

- faulty account management, customer service or collection activities;
- solicitation or referral of customers not meeting **FI**'s risk profile
- inadequate underwriting analysis; and
- poorly structured product programs.[10]

2.5.6. "Other" – risks the **FI** may face arising from the 3rd -party relationship, including

- liquidity, interest rate, price and foreign currency translation, and
- exposure to country risk.[11]

2.6. Additional risks when "outsourcer" is a technological or Internet "start-up."

2.6.1. By contrast to traditional information technology, e.g., mainframe computer services, insufficient time has passed to develop clear "best practices" for Internet services industry.

2.6.2. Management teams for "start-ups" tend to be less experienced, lacking knowledge of what characterizes an "industrial strength" business application.

2.6.3. "start-ups" often must emphasize booking revenue at the expense of sustainability, reliability, security and other indicia of well-developed applications and well-managed services.

2.6.4. Emphasis on reducing "time to market" can lead to further cutting of corners on such indicia.

---

[8] Id., p. 5.
[9] Id.
[10] Id.
[11] Id.

3. Risk Management Process

The OCC has stated that the following risk management principles are essential components of well-structured risk management processes for 3rd-party service provider relationships.

3.1. Risk assessment and strategic planning – Senior management (and the Board) should consider

3.1.1. the role of the 3rd -party relationship in **FI**'s overall business strategy and how relationship and strategy integrate;
3.1.2. whether **FI** has the internal expertise to evaluate and manage the activity and the 3rd -party relationship;
3.1.3. the realism of cost/'benefit relationships, recognizing that the costs of a failed relationship frequently far outweigh any possible benefits; and
3.1.4. how to manage the inevitable customer relationship issues.[12]

3.2. Due diligence in selecting 3rd party – to identify qualitative and quantitative aspects of the 3rd party the **FI** will utilize. This may involve

3.2.1. assessing the experience of the 3rd party and its management in implementing and supporting the proposed activity;
3.2.2. audited financial statements;
3.2.3. adequacy of internal controls, technology recovery; business resumption and contingency operations planning;
3.2.4. reliance on and success in dealing with subcontractors; and
3.2.5. insurance coverage, among other factors.[13]

3.3. Contractual issues – the expectations of the parties should be clearly defined, understood and enforceable. Contracts with the 3rd party should specify, among other topics:

3.3.1. in detail, the scope of the arrangement and its cost and compensation features;
3.3.2. performance measures of benchmarks;
3.3.3. responsibilities for providing and receiving information;
3.3.4. **FI**'s right to audit the 3rd party and consent to oversight by **FI**'s supervisory authority;
3.3.5. ownership of, and rights to use, intellectual property;
3.3.6. requirements for confidentiality and security (see, 6.4.3.2, below);
3.3.7. business resumption and contingency operations planning processes and responsibilities;
3.3.8. rights upon default and at other termination or expiration;
3.3.9. handling of customer complaints; and

[12] Id., p. 7.
[13] Id., p. 9.

3.3.10. special factors attributable to foreign-based service providers.[14]

Separately, the OCC has stated that it will review 3rd party service provider contracts to ensure that they provide for sufficient reporting to allow appropriate evaluation of the 3rd party's performance and security.[15]

3.4. Oversight of relationships – **FI** must monitor the 3rd party's activities and performance, as well as its ongoing financial condition. The OCC provided a substantial checklist of what an **FI** should monitor in monitoring performance.[16]

3.5. Documentation – the **FI** must document its oversight program.[17]

Separately, the Federal Deposit Insurance Corporation ("FDIC") released a "Bank Technology Bulletin on Outsourcing" that contains three reports addressing issues arising in the use of 3rd parties. These reports are not official regulatory guidance but offer practical ideas for banks to consider when they engage in technology outsourcing.[18] The three reports are entitled "Effective Practices for Selecting a Service Provider," "Tools to Manage Technology Providers' Performance Risk: Service Level Agreements," and "Techniques for Managing Multiple Service Providers."

4. Weblinking

The OCC previously had applied many of the foregoing risk management principles in its July 3, 2001 bulletin highlighting the risk of, and providing risk management guidance concerning, banks' weblinking relationships with 3rd parties.[19]

The OCC summarized the guidance in this bulletin with three "key points," i.e., that banks should:

4.1. Conduct sufficient due diligence on the ability of such 3rd parties to which they propose to link to provide service and maintain information security and privacy policies to minimize strategic and reputation.

4.2. Negotiate formal contracts defining the rights and responsibilities of the bank and its weblinking partner to minimize transaction and reputation risk.

---

[14] Id., p. 13.
[15] OCC Bulletin 2001-35, Examination Procedures to Evaluate Compliance with the Guidelines to Safeguard Customer Information, July 18, 2001, Attachment A, part IV. This Bulletin is referred to in these notes as the "Examination Procedures."
[16] OCC Bulletin 2001-47 at 14.
[17] Id., p. 15.
[18] FDIC, Financial Institution Letter FIL-50-2001, Bank Technology Bulletin on Outsourcing, June 4, 2001.
[19] OCC, Bulletin 2001-31, Message to Bankers and Examiners re: Weblinking, July 3, 2001.

4.3. Display appropriate disclosures on the *bank's* website to avoid customer confusion about which entity is providing the services, in order to minimize transaction and compliance risk.[20]

5. Protection of Consumer/Customer Information: Gramm-Leach Bliley Act ("GLBA") Requirements

5.1. One key risk of outsourcing arrangements is that of disclosure of consumer/customer nonpublic information. See 2.5.3, above. In addition to the probable adverse effect on **FI**'s reputation, a significant compliance risk was introduced by GLBA.

5.2. GLBA[21] § 501(a) states that "[I]t is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers *and to protect the security and confidentiality of those customers' nonpublic personal information*."

5.3. GLBA § 501(b) required the federal **FI** regulatory agencies[22] to "establish standards ... relating to administrative, technical and physical safeguards –

5.3.1. "to insure the security and confidentiality of customer records and information;

5.3.2. "to protect against any anticipated threats or hazards to the security or integrity of such records; and

5.3.3. "to protect against unauthorized access to or use of such records or information which could result in substantial harm of inconvenience to any customer."

6. "Interagency Guidelines" re Safeguarding Customer Information

6.1. On June 26, 2000, the federal **FI** regulatory agencies issued for comment "Guidelines Establishing Standards for Safeguarding Customer Information ..."[23] The final rule, published on February 1, 2001,[24] amended the regulations of each

---

[20] Id., at 1.

[21] 12 U.S.C. 6801, et. seq.

[22] The National Credit Union Administration (federally insured credit unions), the Securities and Exchange Commission (brokers and dealers, investment companies, investment advisers), State insurance authorities (persons engaged in providing insurance) and the Federal Trade Commission (any other financial institution) also were required to establish appropriate standards for the financial institutions subject to their respective jurisdictions. GLB Act. § 501(a).

[23] 65 FR 39472 (2000).

[24] 66 FR 8615 (2001).

of the agencies to incorporate the Guidelines.[25] References hereafter are to the Appendix B to 12 C.F.R. Part 30, adopted by OCC.

6.2. Information Security Program

Each **FI** must implement a comprehensive written information security program that implements the objectives of the GLBA (see ¶ 5.3, above).[26]

6.2.1. The program applies to any record containing nonpublic personal information about an **FI** consumer customer[27], whether in paper, electronic or other form.[28] However, the OCC subsequently "encouraged" national banks to extend the information security program to protect all customer and bank records.[29]

6.2.2. The program must apply to physical, as well as electronic, records containing customer information in order to avoid such risks as "identity theft."

6.2.3. Not all parts of the organization, e.g., subsidiaries of a bank holding company, need have a uniform policy, but the policies must be coordinated.

6.3. Involvement By Board of Directors

The Board of Directors or a committee ("Directorate") must:

6.3.1. Approve the written information security program; oversee the development, implementation and maintenance of the program, including assigning specific implementation responsibility and reviewing management reports.[30]

6.3.2. The Directorate of each legal entity in the company, e.g., each bank holding company subsidiary, must carry out these responsibilities independently, although they all may adopt substantially the same program, as long as it complies with the requirements of the entity's primary supervisor.[31]

6.4. Activities in the Information Security Program

6.4.1. Assess Risk[32]

---

[25] For example, the Office of the Comptroller of the Currency amended 12 C.F.R. Part 30 to incorporate an Appendix B that contains the Guidelines.

[26] 12 C.F.R. Part 30, Appendix B, ¶ II.A.

[27] "Customer" has the same meaning as applies in the regulations implementing the privacy provisions of the GLB Act, i.e., a consumer who has a continuing relationship with an **FI** under which the **FI** provides financial products to be used primarily for personal, family or household purposes. (12 C.F.R. Part 40, §§ 40.3(h) and (i)(1)).

[28] 12 C.F.R. Part 30, Appendix B, ¶ I.C.2.c.

[29] OCC Bulletin 2001-8 at 2.

[30] 12 C.F.R. Part 30, Appendix B, ¶ III.A.

[31] 66 F.R. 8620 (2001).

[32] 12 C.F.R. Part 30, Appendix B, ¶ III.B.

6.4.1.1. The risk assessment must cover potential threats to customer information and customer information systems. This is a very broad charter, as "customer information systems" are any methods used to collect, process, store, transmit, protect or dispose of customer information.[33]

6.4.1.2. The **FI** must evaluate the seriousness of these threats in light of the sensitivity of the customer information to be protected.[34]

6.4.2. Manage and Control Risk

6.4.2.1. The **FI** must design its program to control the risks, commensurate with the sensitivity of the information and the complexity and scope of the **FI's** activities.[35]

6.4.2.2. The Guidelines list eight measures that **FI**s must consider in determining their risk control strategy. These measures range from access controls and physical access restrictions through data encryption, change control procedures for information systems, monitoring to detect attacks/intrusions into the systems, response procedures to security breaches and disaster recovery planning.[36]

6.4.2.3. The **FI** must regularly test the key controls. Tests should be conducted or reviewed by independent 3rd parties or independent internal auditors.[37]

6.4.3. Oversee Service Provider Arrangements

FIs must:

6.4.3.1. exercise due diligence in selecting service providers[38], including reviewing the measures taken by the service provider and any subservicer to protect customer information.[39]

6.4.3.2. require service providers by contract to implement appropriate measures designed to meet the objectives of the Guidelines.[40] Contracts entered into starting March 5, 2001 must contain this requirement. All other service provider contracts must be in compliance by July 1, 2003.[41]

The **FI** need not require a service provider to implement the program adopted by the **FI**. Indeed, when the provider services a number of **FI**s, it would likely be impossible to do so. However,

---

[33] 12 C.F.R. Part 30, Appendix B, ¶ I.C.2.d.
[34] 12 C.F.R. Part 30, Appendix B, ¶ III.B.2.
[35] 12 C.F.R. Part 30, Appendix B, ¶ III.C.1.
[36] Id.
[37] 12 C.F.R. Part 30, Appendix B, ¶ III.C.3.
[38] 12 C.F.R. Part 30, Appendix B, ¶ III.D.1.
[39] 66 FR 8624 (2001).
[40] 12 C.F.R. Part 30, Appendix B, ¶ III.D.2.
[41] 12 C.F.R. Part 30, Appendix B, ¶ III.G.2.

each **FI** must satisfy itself that the service provider's program and plan applicable to the **FI** fulfills the objectives of the Guidelines.[42]

6.4.3.3. monitor service provider information security programs to verify compliance, such as by reviewing audits, summaries of test results, etc.[43]

6.4.4. Adjust the Program

FIs must take into account relevant changes in technology, sensitivity of customer information, internal and external threats and the **FI**'s own changing corporate situation.[44]

6.4.5. Report to the Board

FIs must report to their Boards of Directors at least annually.[45]

6.5. Effective Date

6.5.1. The Guidelines became effective March 5, 2001.

6.5.2. **FI**s must have their information security programs in place by July 1, 2001.[46]

6.6. OCC Bulletin 2001-35 contains the examination procedures that the OCC will use to review a national bank's compliance with the Guidelines. The examiners will tailor the examination scope under these procedures according to the size and complexity of the bank. The examination procedures have five substantive parts:

6.6.1. Part 1 – determine the involvement of the Board of Directors, the crux of this part being an assessment whether management and the Board adequately oversee the institution's information security program;

6.6.2. Part II – evaluate the risk assessment program. Does the institution adequately and thoroughly assess risks to its information assets, including vendor oversight requirements?

6.6.3. Part III – evaluate the adequacy of the program to manage and control risk.

7. "Interagency Guidance" re Authentication

7.1. On August 8, 2001 the FFIEC issued guidance on the risks and risk management controls necessary to verify the identity of new customers and to authenticate existing customers accessing electronic financial services.

7.2. Existing authentication methodologies involve three basic "factors":

7.2.1. Something the user *knows*, e.g., password, PIN;

---

[42] 66 FR 8624 (2001).
[43] 12 C.F.R. Part 30, Appendix B, ¶ III.D.3.
[44] 12 C.F.R. Part 30, Appendix B, ¶ III.E.
[45] 12 C.F.R. Part 30, Appendix B, ¶ III.F.
[46] 12 C.F.R. Part 30, Appendix B, ¶ III.G.1.

7.2.2. Something the user *possesses*, e.g., ATM card, smart card; and
7.2.3. Something the user *is*, e.g., biometric characteristics such as a fingerprint or retinal patterns.[47]

7.3. The **FI** must conduct a risk assessment of its electronic banking systems.

7.3.1. The assessment must take into account types of customers (retail, commercial), transactional capabilities (bill payment, wire transfer, loan origination), sensitivity and value of the stored information, ease of using the authentication method under consideration and the size and volume of transactions.[48]

7.3.2. The method of authentication used should be appropriate and "commercially reasonable" in light of the reasonably foreseeable risks in that application. It must be implemented on an enterprise-wide scale. The FFIEC provides a number of examples of the types of authentication systems the industry commonly applies to different types of electronic banking applications.[49]

7.4. The **FI** must conduct account origination and customer verification. This function historically was accomplished by face-to-face communication. In electronic banking applications, other techniques must be used. These include

7.4.1. Positive verification of information the prospect offers to be sure it matches trusted 3rd party sources of information about the prospect.
7.4.2. Logical verification to determine if the information offered by the prospect is internally consistent.
7.4.3. Negative verification to ensure that the information offered has not previously been associated with fraudulent activity.
7.4.4. Reliance on a trusted 3rd party to verify the identity of the prospect. The 3rd party would issue the prospect an electronic credential, e.g., a digital certificate, that the prospect can use to prove identity.[50] (An extended discussion of digital certificates and their possible roles in electronic banking appears in Appendix A.)

7.5. Once an account has been created, the **FI** must authenticate the identity of account users. Available methods for doing so include the use of passwords, PINs, digital certificates, physical devices such as tokens and biometrics.[51]

7.6. Monitoring systems must be in place to detect unauthorized access to computer systems and customer accounts. These systems should include audit

[47] FFIEC, Authentication in an Electronic Banking Environment, July 30, 2001, at 2
[48] Id.
[49] Id., at 3.
[50] Id., at 4.
[51] Id., at 5. In an appendix to the guidance, the FFIEC discusses each of the methods and prudent controls.

logs and other features to detect fraud and unusual activities, unauthorized activities. Other techniques can also be used, e.g., analysis of transactional activity to identify suspicious patters, establishment of dollar limits requiring manual intervention. In addition, reporting mechanisms must be in place regarding cancellation of user account access rights. This must apply to 3rd parties operating the application on behalf of the institution. An independent party should review activity reports to provide the necessary checks and balances for managing system security.[52]

8. Other Regulatory Guidance

The federal **FI** regulators have issued other relevant guidance to **FI**s on the subject of information protection. A sampling of these issuances appears in Appendix B.

[52] Id.

Appendix A

1. Digital signatures are a technology for encrypting digital transmissions. This technology

1.1. ensures that the transmission is not changed en route (integrity),

1.2. provides assurance that the sender actually is who she purports to be (attribution/authenticity), because the public key is included in a "certificate" issued by a trusted third party that is part of the digital signature. The third party issues the certificate to the sender after establishing that she is who she purports to be, and

1.3. makes it very difficult to claim the transmission was sent by an impostor (non-repudiation).

With the addition of a date-stamp on the transmission, the time of sending can be established, as well.

2. The technology (sometimes called "public key infrastructure" or "PKI") achieves these objectives in large part by

2.1. encrypting certain unique information about the transmission, including, sometimes, the message itself, with a secret, "private key" known only to the sender;

2.2. including in the encrypted transmission a "message digest," created by the sender, that is unique to the particular transmission;

2.3. requiring use of the sender's "public key," which may be widely publicized, to decrypt the transmission; and

2.4. recalculating the "message digest," to verify that it is the same as the sender inserted in the transmission.

3. This encryption/decryption relationship achieves the three characteristics described above (¶ 1) by

3.1. verifying the "message digest." If the transmission has been altered in any way en route, the "message digest" calculated by the receiver will not be the same as that created by the sender,

3.2. relying on the certification by the trusted third party that the sender is who she purports to be, and

3.3. determining that the sender's private key has not been compromised, so that only the sender could have encrypted the transmission.

4. Digital signatures provide high security for transmissions. No doubt, their use would fulfill any direction of the Guidelines to encrypt (see ¶ 6.4.2.2, above). However, PKI systems are expensive and complex to create, manage and use. As a general mechanism for ensuring security of information transmitted, they may be "overkill" at this stage in their development.

5. However, digital signatures solve some practical problems arising in the use of electronic signatures in e-commerce transactions.

Appendix B

1. **OCC** Bulletin 2000-14, Infrastructure Threats – Intrusion Risks. Provides guidance on how to prevent, detect and respond to intrusions into bank computer systems. (May 15, 2000)
2. **OCC** Advisory Letter 2000-12, Risk Management of Outsourcing Technology Services. Transmits guidance from the Federal Financial Institutions Examination Council ("FFIEC") outlining the processes banks should use to manage the risks associated with outsourcing technology. (November 28, 2000)
3. **OCC** Bulletin OCC 99-20, Certificaton Authority Systems. Identifies the risks of certification authority systems. (May 4, 1999)
4. **OCC** Banking Circular BC-229, Information Security. Alerts management to the importance of information security. (May 31, 1998)
5. **OCC** Bulletin OCC 98-3, Technology Risk Management. Provides guidance on how national banks should identify, measure, monitor and control risks associated with the use of technology. (February 4, 1998)
6. **OCC** Banking Circular BC-226, End-User Computing. Transmits a joint issuance of the FFIEC on risks associated with end-user computing activities. (January 25, 1988)
7. **OCC** Advisory Letter AL 96-1, Document Security. Discusses appropriate procedures to ensure the security of confidential documents. (March 15, 1996)
8. **OCC** Banking Circular BC-187, Financial Information on Data Servicers Processing. Alerts national banks to the importance of performing financial reviews of organizations providing data processing services. (January 18, 1985)
9. BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM ("**FRB**"), Supervisory Letter, SR 00-4(SUP), Outsourcing of Information and Transaction Processing. (February 29,2000).
10. FEDERAL DEPOSIT INSURANCE CORPORATION ('**FDIC**"), Financial Institution Letter FIL-67-2000, Security Monitoring of Computer Networks. (October 3, 2000)
11. **FDIC**, Financial Institution Letter FIL-131-97, Security Risks Associated with the Internet. (December 18, 1997)
12. OFFICE OF THRIFT SUPERVISION ("**OTS**"), Memorandum, Transactional Web Sites. Provides information on regulatory requirements for transactional web sites. (June 10, 1999)
13. **OTS**, Memorandum, Policy Statement on Privacy and Accuracy of Personal Customer Information. Set out "best practices" to adequately protect personal information. (November 3, 1998)
14. **OTS**, Memorandum, Statement on Retail On-Line Personal Computer Banking. Alerts to some of the risks and concerns of retail on-line PC banking. (June 23, 1997)

15. **OTS**, Memorandum, Risk Management of Client/Server Systems. Encourages development and implementation of sound policies, practices and procedures to mitigate risks posed by a client/server environment. (October 24, 1996)